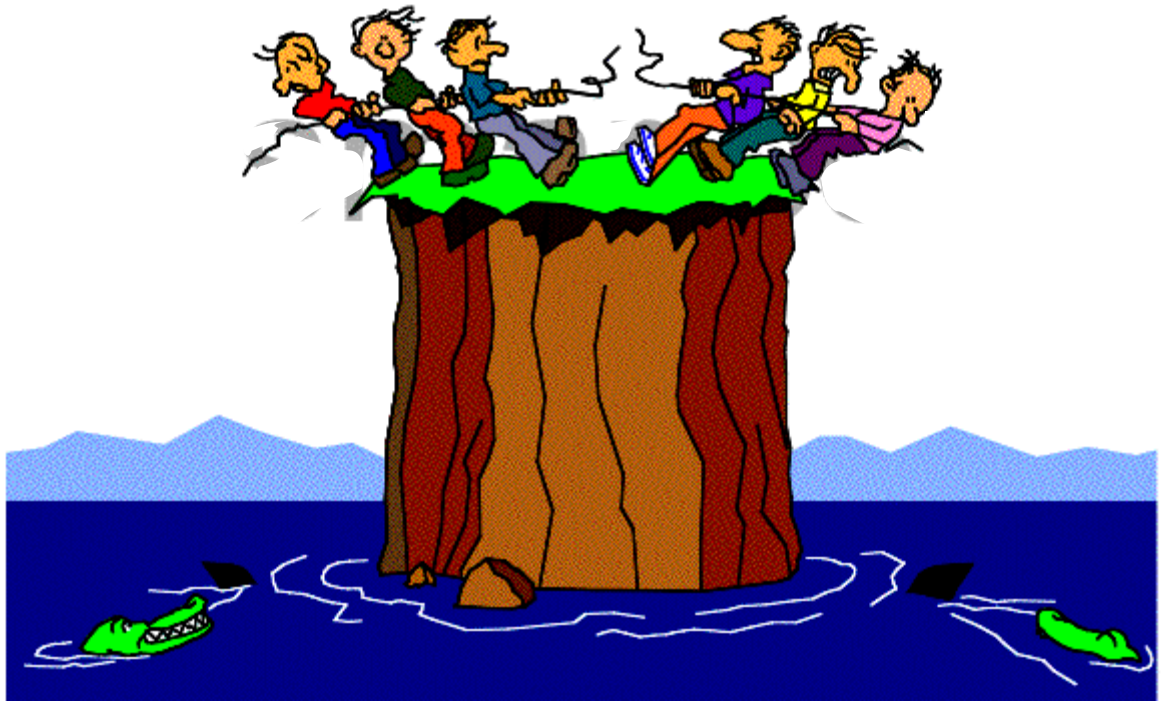
Auditi läbiviimine



Auditi plaan pole kivist

- Pole olnud audit, mis oleks toimunud täpselt plaani järgi

Esimene (ava-) kohtumine

- Tutvusta auditi tiimi osakonna töötajatele
- Kirjelda (veelkord) auditi toimumise aega, kestust ja skoopi
- Lepi kokku ametlik suhtlemisviis
- Esita dokumentide ülevaatuse leiud

Oluline (primaarne) mittevastavus (*Major nonconformance*)

- Süsteemi täielik (totaalne) mittevastavus standardile
- Ühe nõude puhul on (liiga) suur arv mitteolulisi mittevastavusi, mis kummulatiivselt viivad süsteemi krahhile

Sekundaarne (väheoluline) mittevastavus (*Minor nonconformance*)

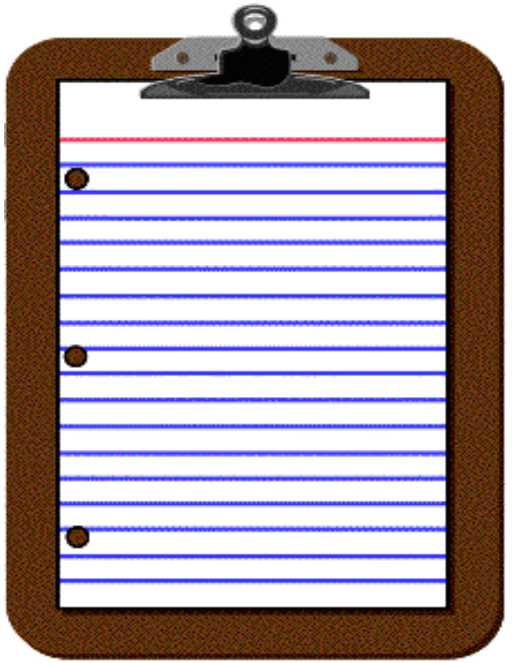
- Mittevastavus, mis ei tingi süsteemi krahhi

Tähelepanek (*Observation*)

- = audiitori arvamus
  - Traditsiooniline interpretatsioon: korrigeeriv toiming pole vajalik
  - KUID!!! Mõnedel audiitoritel on TÄHELEPANEK intepreteeritud erinevalt
    - Näiteks: audiitor teebki ainult tähelepanekuid (olulisi, mitteolulisi, teisejärgulisi jne)

Auditi kulg

- Selgita, millega tahad tutvuda, mida näha
- Ära eelda, et “PAHA” on olemas
- Ära ole pettunud järelduse “Probleeme pole” puhul
- Kasuta oma kontroll-listi juhendi-plaanina
- Tee märkmeid (ära usalda oma mälu):
  - Antud auditi tarvis
  - Järgnevate audite tarvis
  - Teiste audiitorite tarvis
- Iga tähelepaneku jaoks:
  - Ignoreeri (aruandes)
  - Fikseeri (arundes)
  - Märgista järelkontrolli vajavaks (*later follow-up*)
  - Pöördu osakonna juhataja/teiste spetsialistide poole selgituse saamiseks



Head tavad auditeerimisel

- Teavita eelnevalt – pole vaja üllatusi
- Selgita probleemi olulisust
- Avalikusta kohe tulemused – midagi pole vaja varjata
- Ära unusta, et audit põhjustab stressi!
- Esita küsimused “õigele” inimesele
  (“õiged” on need, kes teevad)
- Räägi lihtsalt ja selgelt, ära “räägi surnuks”
- Hoidu emotsionaalsusest
- Ära katkesta auditeeritavat, ära räägi vahele
- Ära otsi puudusi

Halvad tavad auditeerimisel

- Esitada liiga palju küsimusi
- Esitada suunavaid küsimusi
- Öelda, et saad aru, kui ei saanud
- Vastata ise oma küsimustele
- Provotseerida vaidlust
- Olla erapoolik
- Kritiseerida isikuid

Tõendite kogumine

- Intervjueeri personali
- Analüüsi dokumentatsiooni
- Fikseeri tähelepanekud tingimustest ja toimingutest
- Dokumenteeri vastavused
- Dokumenteeri mittevastavused, märkides ära
  - Miks on tegemist mittevastavusega
  - Kus leiti
  - Kes osales(id)
  - Objektiivsed tõendid
  - Viited standarditele

Mittevastavus eksisteerib kuna ...

- Süsteem ei vasta standardi(te)le, protseduuridele või teistele nõuetele
- Teostus ei vasta süsteemile
- Teostus pole tõhus

Mittevastavuste gradatsioon

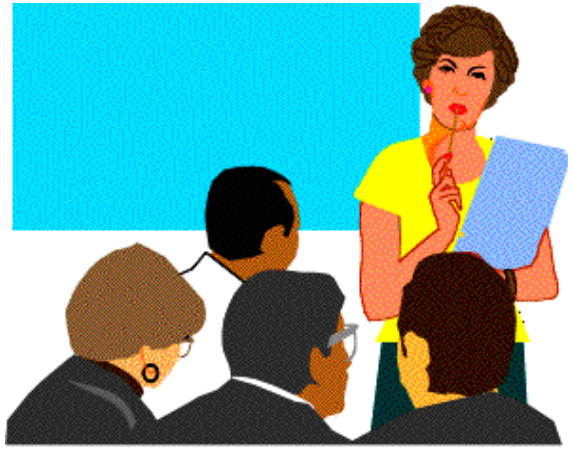
- **Olulised (*major*)**
  - Standardi mingit osa on ignoreeritud
  - Võib põhjustada mittevastava toote/teenuse väljastamise
  - Protseduur, mida regulaarselt on ignoreeritud
- **Väheolulised, sekundaarsed (*minor*)**
  - 3 kuni 5 VÄHEOLULIST ühes süsteemis/protsessis *võib* anda OLULISE mittevastavuse
- **Leiud (*findings*)**
  - Väheoluline probleem, üksik intsident
  - Leiule peab auditeeritav reageerima
- **Tähelepanek (*observation*)**
  - Võimalus süsteemi/protsessi parendada

Mittevastavuste gradatsioon: KÜSIMUSED

- Mis juhtub süsteemiga, kui mittevastavust ei korrigeerita?
- Missugune on halva stsenaariumi tõenäosus?
- Kas võib juhtuda, et mittevastav toode/teenus jõuab lõppkasutajani?

Kokkuvõttev kohtumine (*Closing Meeting*)

- Tänud kõigile!
- Allkirjad osalejatelt
- Ülevaade auditi eesmärkidest ja skoobist
- Piirangud
- Mis oli positiivset – see kõigepealt!
- Leidude loetelu
- Küsimused ja vastused. Konsensus.
- Kokkuvõte – mitte unustada konsensust
- Aitäh!



Mittevastavuste aruanne

Meelespea

- Ole konkreetne
  - Kus
  - Mis
    - Nimi
    - Number
  - Miks
    - Süsteem
    - Protseduur
- Kontrolli fakte!

Kokkuvõte

- Mittevastavuste arv
- Mittevastavuste asukoht
- Toimingud, kus mittevastavusi ei leitud
- Enamlevinud mittevastavuste tüübid
- Soovitused

Mis välja jätta

- Mitteolulised detailid
- See, millest ei räägitud
- Konfidentsiaalsed andmed
- Ebamäärased väited/avaldused
- Audiitori (sinu) arvamus

Korrigeerivad toimingud

- Auditeeritav kavandab toimingud leitud mittevastavuste korrigeerimiseks (vastutaja, tähtaeg)
- Auditeeritav vastutab korrigeerivate toimingute plaanimise, teostamise ja seire eest

Auditi järelkontroll

- Hinnang korrigeerivale toimingule
- Vastus: kes, mida, millal, kuidas
- Vastuse hinnang
- Dokumentatsiooni ülevaatus
- Korrigeeriva toimingu kinnitus
- Järeldus

Järelkontroll

- Enam detailne
- Variatsioonid

Siseaudit

Siseauditi mõiste

Siseaudit on **SÕLTUMATU** ja objektiivne, kindlustandev ning **KONSULTEERIV** tegevus, mis on suunatud ettevõtte **TEGEVUSE TÄIUSTAMISEKS** ja väärtuse lisamiseks.

Ta aitab kaasa asutuse **EESMÄRKIDE SAAVUTAMISELE**, kasutades süsteemset ja distsiplineeritud lähenemist, hindamaks ja täiustamaks riskide juhtimise, kontrolli ja valitsemiskultuuri efektiivsust.

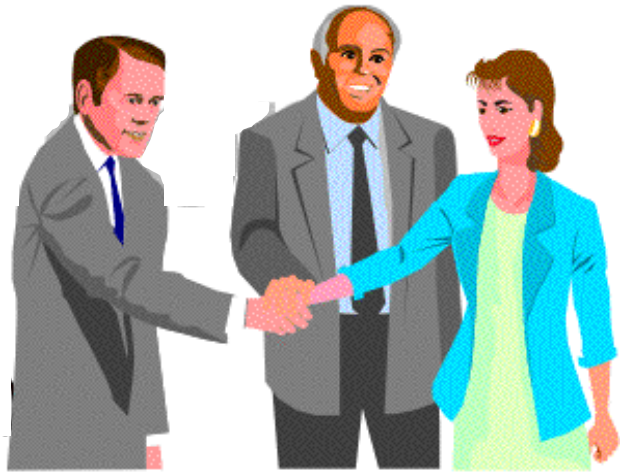
The Institute of Internal Auditors (1999.a)

Mida peab arvestama siseaudit?

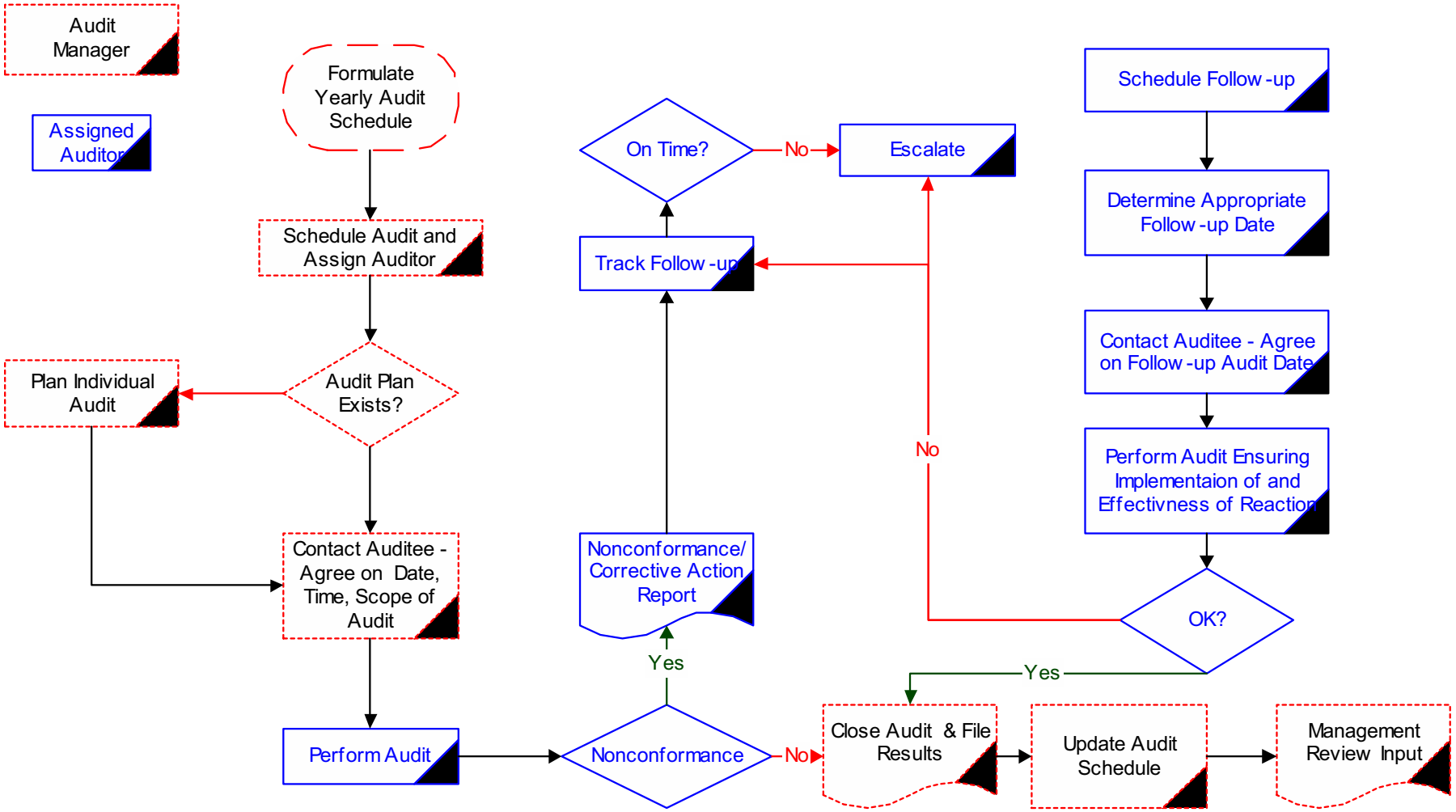
- Siseauditil peab olema aastaplaan
- Siseaudit nõuab tõhusaid korrigeerivaid toiminguid
  - mõned mittevastavused ei nõua korrigeerivaid toiminguid
  - mõned mittevastavused nõuavad minimaalseid korrigeerivaid toiminguid
  - mõned mittevastavused nõuavad põhjalikke korrigeerivaid toiminguid
- Siseaudit verifitseerib korrigeerivaid toiminguid
- Siseauditi aruanne annab juhatusele ülevaate ettevõtte riskidest

Siseauditi roll

- Katalüsaator
- Liides erinevate üksuste ja gruppide vahel
- Nõuandja
- Oluliste sündmuste registreerija



Example of Internal Audit System



Siseauditi tegevuse alused

A. KREDIIDIASUTUSTE SEADUS

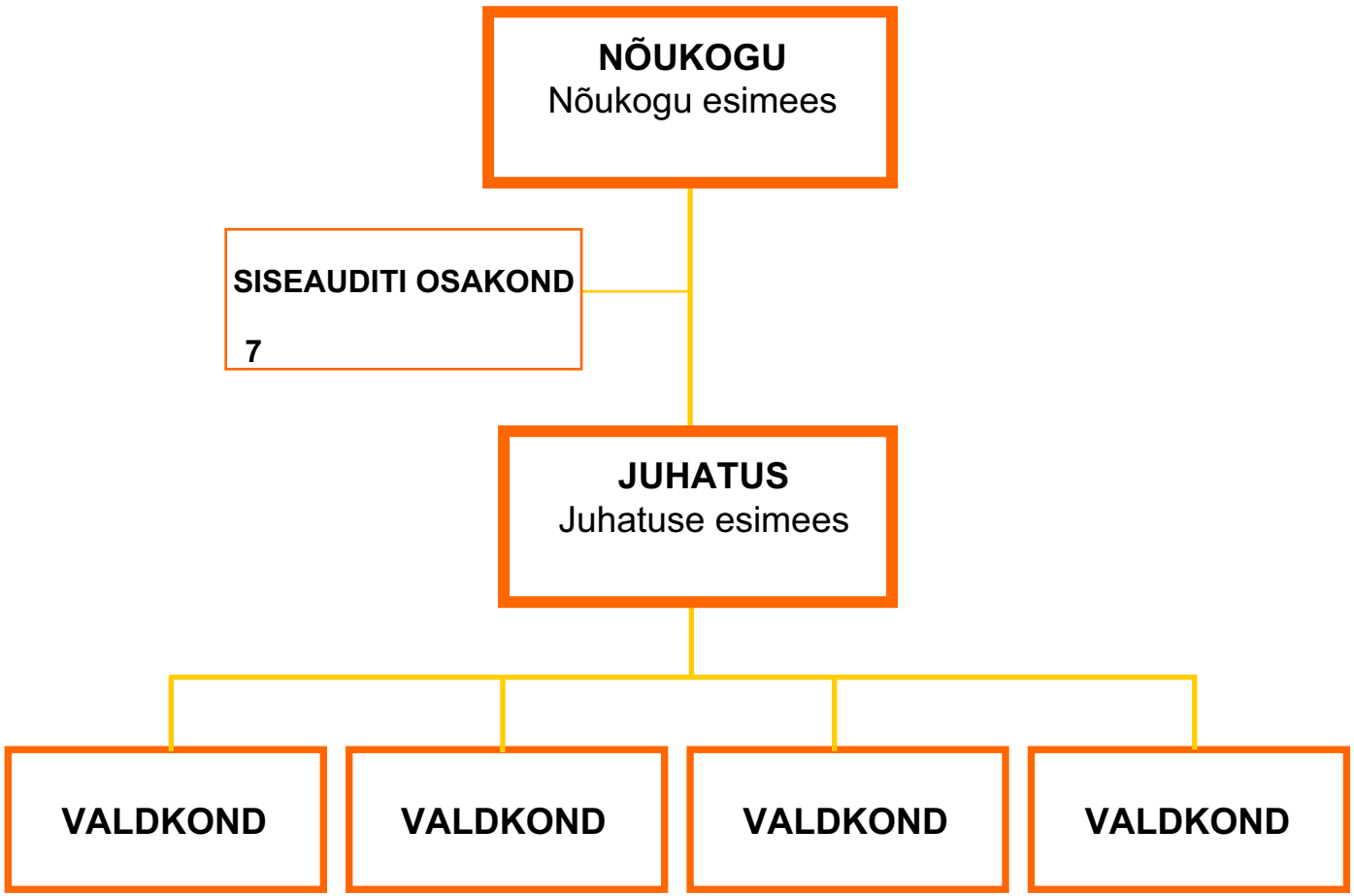
- **Krediidiasutuse sisekontrolli süsteemi osana moodustatakse sõltumatu siseauditi üksus, mis jälgib kogu krediidiasutuse tegevust.**
- **(1) Siseauditi üksus tegutseb krediidiasutuse** NÕUKOGU **poolt kinnitatud põhimääruses sätestatud korras.**
- **(2) Siseauditi üksuse töötajatel on** ÕIGUS JÄLGIDA **piiranguteta krediidiasutuse tööd ning osaleda juhatuse ja krediidiasutuse põhikirja alusel moodustatud komiteede koosolekutel.**
- **(3) Siseauditi üksusel on** ÕIGUS NÕUDA **krediidiasutuse töötajatelt nende tegevuses ilmnenud puuduste ja eksimuste kohta kirjalikke seletusi ning ilmnenud puuduste kõrvaldamist.**

Sisekontroll ja siseauditi osa selles

KREDIIDIASUTUSTE SEADUS (**§55**)

- Krediidiasutuse juhatus (LOE: JUHTKOND) on kohustatud
  - töötama välja ning **RAKENDAMA** asutuse tegevuse kontrollimise süsteemid, tagama nende järgimise, **PIDEVALT HINDAMA** nende piisavust ning vajadusel neid **TÄIUSTAMA**;
  - korraldama sisekontrolli süsteemi tõhusa toimimise;
- Sisekontrolli süsteem **peab hõlmama kõiki krediidiasutuse juhtimistasandeid, et tagada tegevuse** EFEKTIIVSUS**, finants-aruandluse** USALDATAVUS **ning** VASTAVUS **seadustele ja krediidiasutuse juhtkonna poolt kinnitatud dokumentidele.**
- Krediidiasutuse sisekontrolli süsteemi osana **moodusta-takse sõltumatu** SISEAUDITI ÜKSUS**, mis jälgib kogu asutuse tegevust.**

Näide


NÕUKOGU
Nõukogu esimees
SISEAUDITI OSAKOND
7
JUHATUS
Juhatuse esimees
VALDKOND
VALDKOND
VALDKOND
VALDKOND

COSO sisekontrolli definitsioon

Sisekontroll on protsess, mis on loodud tagamaks piisavat kindlust järgmiste eesmärkide saavutamisel:

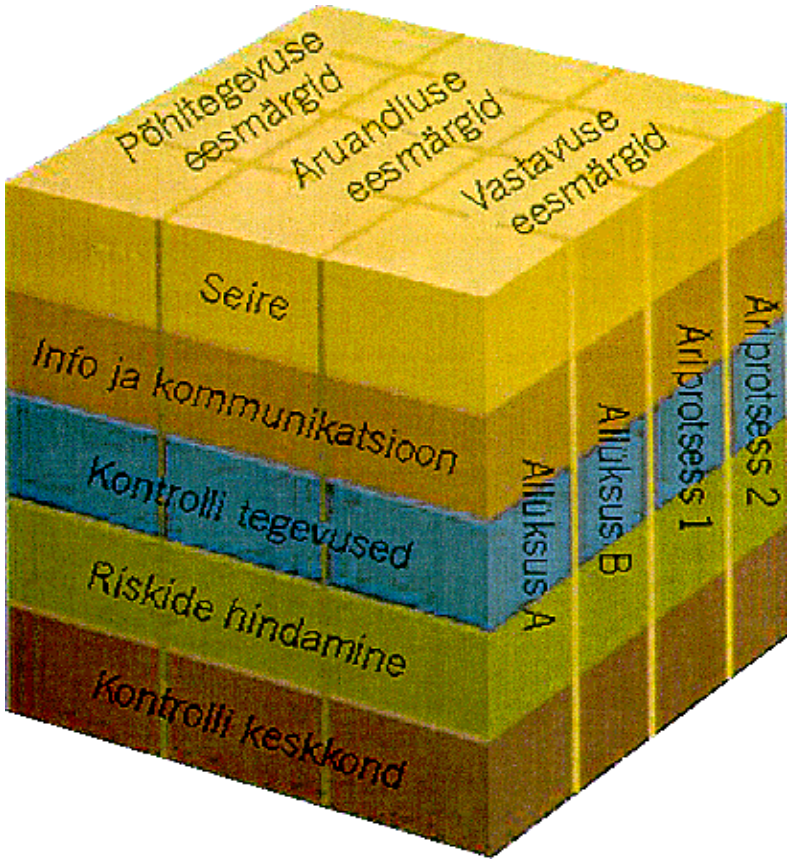
- **Äriprotsesside toimivus ja efektiivsus**
- **Finantsaruandluse usaldusväärsus**
- **Vastavus seadustele ja muudele normatiivaktidele**

Võtmekontseptsioonid:

- **Sisekontroll on protsess. See on vahend eesmärgi saavutamiseks, mitte eesmärk ise.**
- **Sisekontrolli viivad läbi inimesed. See ei koosne ainult poliitikatest ja kordadest, vaid** INIMESTEST **igal organisatsiooni tasandil.**
- **Sisekontroll ei taga eesmärgi saavutamisel absoluutset kindlust**

Sisekontrolli süsteem

- COSO (http://www.coso.org/) kuubik sisekontrolli süsteemi komponentidest



Sisekontrolli süsteemi komponendid

- KONTROLLIKESKKOND

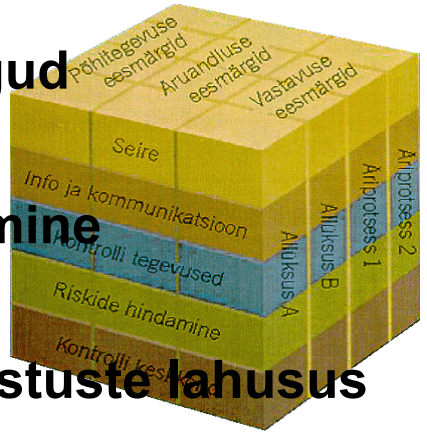
  Seadusandlus, tööjõupoliitika, väärtushinnangud

- RISKIDE HINDAMINE

  Keskendumine olulisele, ressursside planeerimine

- KONTROLLTEGEVUSED

  Kinnitused, autoriseerimised, võrdlused, kohustuste lahusus



- INFO JA KOMMUNIKATSIOON

  Regulaarne info kontrolltegevuste toimumise, protsessi- ja keskkonna-muudatuste ning erandite kohta. Info liikumine organisatsioonis ülevalt alla ja alt üles. Kommunikatsioonis väljendub iga töötaja arusaamine tema osast sisekontrollisüsteemis.

- SEIRE

  Sisekontrollisüsteemi sõltumatu hindamine - audit

Sisekontrollide liigid ja tehnikad

Liigitamine ajalises dimensioonis

- Suunavad kontrollid
  (korrad, reeglid)
- Ennetavad kontrollid
  (süsteemsed kontrollid, eelmisest tegevusest sõltuvad kontrollid, kohustuste lahusus)
- Järelkontrollid
  (aruandlus, inventuurid, auditi jälje analüüsid)

Liigitamine eesmärgi alusel

- Andmete käideldavusele
- Andmete terviklikkusele
- Konfidentsiaalsusele

suunatud kontrollid

Liigitamine toimimis-keskkonna alusel

- Manuaalsed kontrollid
- Süsteemsed kontrollid

Siseauditi töökorraldus

1. **Siseaudiitorid töötavad juhatusega ja välisaudiitoritega kooskõlastatud ja nõukogu poolt kinnitatud TÖÖPLAANI ALUSEL**
2. **Auditite eesmärk on testida oluliste SISEKONTROLLIDE TOIMIMIST läbi erinevate organisatsiooni tasandite, kontrollides grupi töötajate toimingute vastavust kehtestatud reeglitele ja grupi huvidele**
3. **Auditid lõpetatakse RAPORTIGA, mis on läbi arutatud ja allkirjastatud auditeeritud valdkonna eest vastutava juhiga.**
4. **Auditite käigus tehtud TÄHELEPANEKUTE kõrvaldamiseks lepitakse kokku tähtajad ning määratakse töötajad, kes vastutavad lahenduste leidmise ja rakendamise eest**
5. **Siseaudit viib läbi JÄRELKONTROLLE tähelepanekutele reageerimise tulemuste fikseerimiseks**

Siseauditi tööplaan

- Siseauditi osakonna tööplaani aluseks on auditeeritava valdkonna tegevuse riskianalüüs
- Riskianalüüsi koostamisel
  a) Moodustatakse loetelu valdkonna protsessidest
  b) Hinnatakse iga üksiku protsessi riski vastavalt kehtivale metoodikale
  c) Omistatakse protsessidele riskitasemed: kõrge, keskmine ja madal
- Tööplaan koostamisel järgitakse põhimõtet, et
  a) Kõrge riskiga protsesse auditeeritakse 1x aastas
  b) Keskmise riskiga protsesse auditeeritakse vähemalt 1x kahe aasta jooksul
  c) Madala riskiga protsesse auditeeritakse vähemalt 1x kolme aasta jooksul

Performing COBIT Based Audit

COBIT Domains

Planning and Organization	Acquisition and Implementation	Delivery and Support	Monitoring
PO1 – Define a strategic IT plan	**AI1** – Identify automated solutions	**DS1** – Define and manage service levels	**M1** – Monitor the processes
PO2 – Define the information architecture	**AI2** – Acquire and maintain application software	**DS2** – Manage third-party services	**M2** – Assess internal control adequacy
PO3 – Determine the technological direction	**AI3** – Acquire and maintain technology infrastructure	**DS3** – Manage performance and capacity	**M3** – Obtain independent assurance
PO4 – Define the IT organization and relationships	**AI4** – Develop and maintain procedures	**DS4** – Ensure continuous service	**M4** – Provide for independent audits
PO5 – Manage the IT investment	**AI5** – Install and accredit systems	**DS5** – Ensure systems security	
PO6 – Communicate management aims and direction	**AI6** – Manage changes	**DS6** – Identify and allocate costs	
PO7 – Manage human resources		**DS7** – Educate and train users	
PO8 – Ensure compliance with external requirements		**DS8** – Assist and advise customers	
PO9 – Assess risks		**DS9** – Manage the configuration	
PO10 – Manage projects		**DS10** – Manage problems and incidents	
PO11 – Manage quality		**DS11** – Manage data	
		DS12 – Manage facilities	
		DS13 – Manage operations	

Risk Assessment

	Control Risk	Control Evaluation	Effectiveness	Efficiciency	Confidentiality	Integrity	Availibility	Compliance	Reliability
	Materiality		4	4	4	1.5	1.5	1.5	1.5
Planning and organisation									
PO 1	Define a strategic IT plan	2	C	H					
PO 2	Define the information architecture	1	E	C	C	O			
PO 3	Determine the technological direction	2	C	H					
PO 4	Define organisation and relationships	2	C	H					
PO 5	Manage the investment	2	C	C					O
PO 6	Communicate management aims and direction	1	E					O	
PO 7	Manage human resources	1	E	E					
PO 8	Ensure compliance with external requirements	1	E					c	O
PO 9	Assess risk	1	C	C	E	c	c	O	O
PO 10	Manage projects	1	E	E					
PO 11	Manage quality	1	E	E		c			O
Acquisition and implementation									
AI 1	Identify automated solutions	1	E	C					
AI 2	Acquire and maintain application software	1	E	E		O		O	O
AI 3	Acquire and maintain technology architecture	1	E	E		O			
AI 4	Develop and maintain procedures	1	E	E		O		O	O
AI 5	Install and accredit systems	1	E			O	O		
AI 6	Managing changes	2	C	C		c	c		O
Delivery and support									
DS 1	Define service levels	1	E	E	C	O	O	O	O
DS 2	Manage third-party services	1	E	E	C	O	O	O	O
DS 3	Manage performance and capacity	1	E	E			O		
DS 4	Ensure continuous service	2	C	H			c		
DS 5	Ensure systems security	2			C	c	O	O	O
DS 6	Identify and allocate costs	1		E					c
DS 7	Educate and train users	1	E	C					
DS 8	Assist and advice customers	1	E						
DS 9	Manage the configuration	1	E				O		O
DS 10	Manage problems and incidents	1	E	E			O		
DS 11	Manage data	2				c			
DS 12	Manage facilities	2				c	c		
DS 13	Manage operations	1	E	E		O	O		
Monitoring									
M 1	Monitor the process	1	E	C	C	O	O	O	O
M 2	Assess internal control adequacy	1	E	E	C	O	O	O	O
M 3	Obtain independent assurance	1	E	E	C	O	O	O	O
M 4	Provide for Independent Audit	1	E	E	C	O	O	O	O

Legend:				
E	Exposure	H	Housekeeping	
C	Concern	O	OK	
		c	concern +	

COBIT Process	Executives	Finance	IT/IS
Planning and Organization			
PO1 – Define a strategic IT plan	Manage		Control
PO2 – Define the information architecture			Manage/Control
PO3 – Determine the technological direction	Manage		Control
PO4 – Define the IT organization and relationships			Manage/Control
PO5 – Manage the IT investment		Manage	Control
PO6 – Communicate management aims and direction	Manage	Control	Control
PO7 – Manage human resources	Manage/Control		
PO8 – Ensure compliance with external requirements	Manage	Control	Control
PO9 – Assess risks	Manage	Control	Control
PO10 – Manage projects		Control	Manage/Control
PO11 – Manage quality			Manage/Control
Acquisition and Implementation			
AI1 – Identify automated solutions		Control	Manage/Control
AI2 – Acquire and maintain application software	Manage	Control	Manage/Control
AI3 – Acquire and maintain technology infrastructure	Manage	Control	Manage/Control
AI4 – Develop and maintain procedures			Manage/Control
AI5 – Install and accredit systems	Manage		Manage/Control
AI6 – Manage changes			Manage/Control
Delivery and Support			
DS1 – Define and manage service levels	Manage/Control		
DS2 – Manage third-party services	Manage/Control		
DS3 – Manage performance and capacity			Manage/Control
DS4 – Ensure continuous service	Manage/Control		Control
DS5 – Ensure systems security			Manage/Control
DS6 – Identify and allocate costs	Manage	Control	
DS7 – Educate and train users	Manage/Control		
DS8 – Assist and advise customers	Manage/Control		
DS9 – Manage the configuration			Manage/Control
DS10 – Manage problems and incidents			Manage/Control
DS11 – Manage data		Control	Manage/Control
DS12 – Manage facilities	Manage/Control		Control
DS13 – Manage operations	Manage/Control		Control
Monitoring			
M1 – Monitor the processes		Control	Manage/Control
M2 – Assess internal control adequacy	Manage	Control	
M3 – Obtain independent assurance	Manage	Control	
M4 – Provide for independent audits	Manage	Control	

Approach: Phase 1

Phase 1: Pre-Assessment

- Define scope and objectives
  - Identify regulations to comply (e.g. Basel II)
  - Determine relevant control objectives within the CobiT
- Framework
  - Identify approaches (best practice or standard) to improve the identified CobiT control objectives (processes)
  - Tailor questionnaire to specific needs

Phase 2: Assessment

COBIT Domain	COBIT Control Objectives	ITIL-Process	Topic	Controll Questions
Delivery & Support				
1.1	(All) (Top 10...) (Custom...) 1.5 Review of Service Level Agreeme 1.6 Chargeable Items 1.7 Service Improvement Programme 10.1 Problem Management System 10.2 Problem Escalation 10.3 Problem Tracking and Audit Trail 10.4 Emergency and Temporary Acce 10.5 Emergency Processing Priorities 6.1 Change Request Initiation and Co 6.2 Impact Assessment 6.3 Control of Changes 6.4 Emergency Changes 6.5 Documentation and Procedures 6.6 Authorised Maintenance 6.7 Software Release Policy 6.8 Distribution of Software 8.1 Help Desk			
1.1.1.1		Service Level Management	1. Policy & Procedures	Has the IT defined a global policy for SLM containing
1.1.1.1.1		Service Level Management	1. Policy & Procedures	
1.1.1.1.2		Service Level Management	1. Policy & Procedures	
1.1.1.2		Service Level Management	1. Policy & Procedures	Is that formal process accessable?
1.1.1.3		Service Level Management	1. Policy & Procedures	
1.1.1.4		Service Level Management	8. SLA	Defining service /Templates?
1.1.1.4.1		Service Level Management	8. SLA	
1.1.1.4.2		Service Level Management	8. SLA	
1.1.1.5		Service Level Management	8. SLA	Contracting the service / Templates
1.1.1.5.1		Service Level Management	8. SLA	
1.1.1.5.2		Service Level Management	8. SLA	
1.1.1.5.3		Service Level Management	8. SLA	
1.1.1.5.4		Service Level Management	8. SLA	
1.1.1.5.5		Service Level Management	8. SLA	

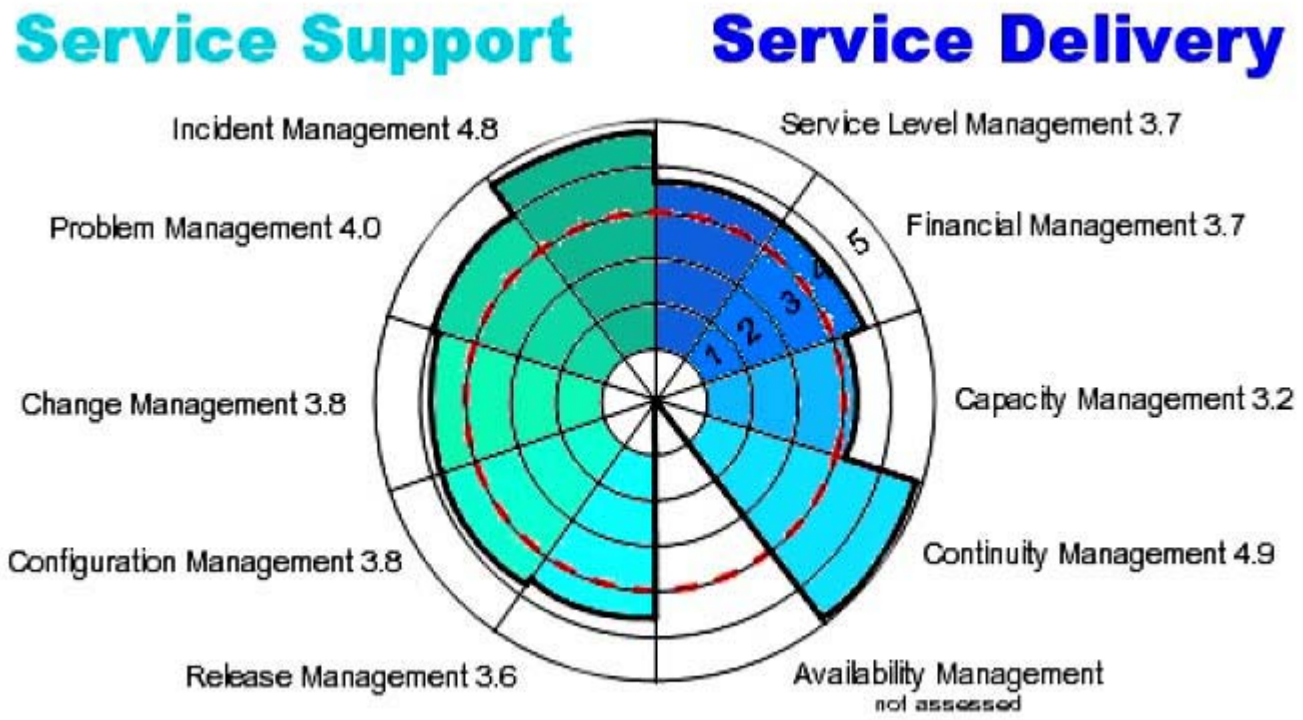
Phase 2: Assessment

ITIL-Process	Topic	Controll Questions	additional questions
Service Level Management	1. Policy & Procedures	Has the IT defined a global policy for SLM containing	Process description
Service Level Management	1. Policy & Procedures		Described activities
Service Level Management	1. Policy & Procedures		Roles & responsibilities
Service Level Management	1. Policy & Procedures	Is that formal process accessable?	
Service Level Management	1. Policy & Procedures		If yes, in where?
Service Level Management	8. SLA	Defining service /Templates?	
Service Level Management	8. SLA		Business requirements
Service Level Management	8. SLA		Service description
Service Level Management	8. SLA	Contracting the service / Templates	
Service Level Management	8. SLA		Service specification sheet
Service Level Management	8. SLA		Service Level Agreement
Service Level Management	8. SLA		Service Catalogue
Service Level Management	8. SLA		Operational Level Agreement
Service Level Management	8. SLA		Underpinning contract

Phase 3: GAP-Analysis

- Rating of assessed processes
- Aggregation of results according to customers requirements
- Comparison of results against standards or/and best practices
- Identification of GAPs between As-Is Situation and selected standards or/and best practices

Phase 3: GAP-Analysis - Overview



Phase 3: GAP-Analysis - Details

ITIL Core requirements for Service Level Mgt:

- Build up a good & stable customer relationship
- Define standard procedures to gather customer requirements
- Define a Sevice catalogue and SLA‘s based on the service specsheet
- Elaboration and support of all SLA‘s, OLA‘s and UC‘s
- Ongoing Control & review of SLAs,OLAs & UCs in order to improve services

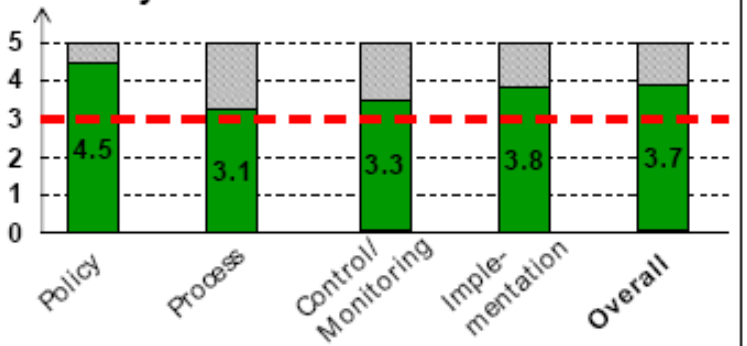
Gaps between As-Is and To-Be (Gap)

- Unclear process definition on how to create, maintain and enforce SLA
- Missing Roles and Responsabilities Matrix
- Review of SLA‘s and OLA‘s not formal
- OLA‘s and 3rd party contracts are not in line with the SLA‘s
- Interfaces towards other processes are not available or not defined, missing templates.

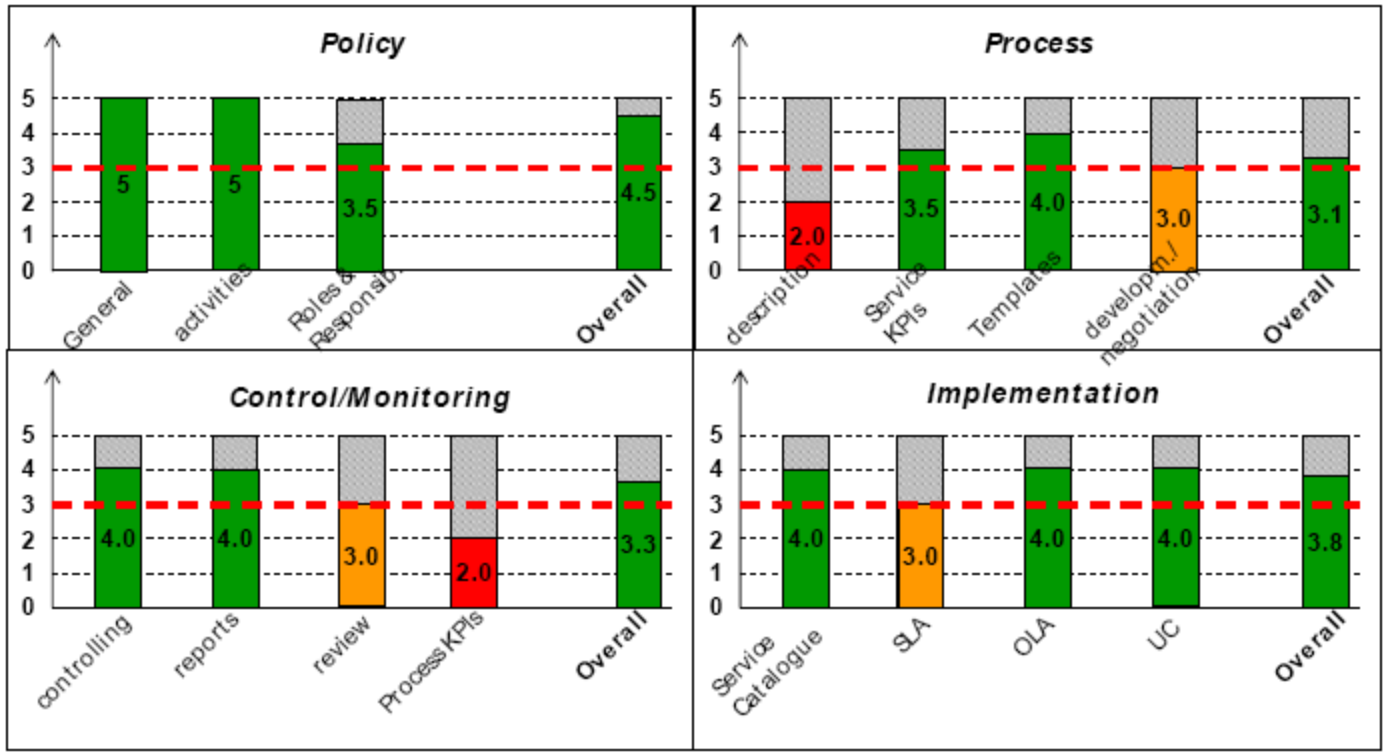
Actions:

- Define and enforce a clear process on how to create SLA‘s
- Define and distribute a complete „roles and responsabilities matrix“ for the Service Level Management Area
- Create a checklist for the review of SLA‘s and OLA‘s and 3rd party contracts.
- When negotiating new contracts, align them with existing SLA‘s
- Clear definition of all Interfaces between ITIL core proscesses

Summary of the results:



Phase 3: GAP-Analysis - Details



Phase 4: Report - Contents

- Management Summary
- Scores Achieved
- Key Findings and Recommendations (Quick Wins)
- Recommended Improvement Projects
- Action List

Phase 4: Report - Action List

Nr.	Module	Title	Gap	Action	Priority	Project
1.1	Incident Management	Policy General	The relation to the Knowledge Management should be defined clearly (e.g. Self Service for Customers etc.).	Define relation towards Knowledge Management	3	General Poli
1.2	Incident Management	Roles	All roles involved in the process have to be described in the policy.	Responsibilities of Service Desk Agent, Knowledge Manager and 2nd Level Support should be defined precisely in the policy as it has been done for the Incident Manager.	1	Interfaces ar Roles
1.3	Incident Management	Prioritization	The prioritization concept that is implemented in Service Centre is not completely documented.	Prioritization should be clearly defined in the policy including max. Resolution Time as well as max. Escalation Time (horizontal and vertical) for each priority	2	Prioritization
1.4	Incident Management	Monitoring/ Control	The Monitoring and Control process has to be defined explicitly.	The monitoring and control process has to be defined which includes responsibility for reporting and derived actions, a list of recipients for the reports. The existing report for Incident Management should contain explanations of the reported values (e.g. why a certain number decreased or increased). Diagrams without any comments should be avoided. Some report information could be made public for all customers as a "marketing instrument". All KPIs should be defined in the Incident Management Policy including a description of the calculation/measurement model as well as the responsibility for measurement etc. Ranges for KPIs should be defined (min/max values).	2	General Poli

Main Benefits of an Assessment

- Quick analyse of actual situation (health check of organisation)
- Only limited efforts, especially for internal resources
- Comprehensive list of concrete defined actions to improve actual situation
- Highly adaptable to specific customer requirements

IS audit: riski tõendamine

Riskihindamise metoodika

- **Operatsiooniriski definitsioon -** Kahju võimalikkus nii väliste (nagu loodusõnnetused, väline kuritegevus) kui sisemiste tegurite (nagu katkestus IT süsteemides, pettus, seadustest ja sisemistest protseduuridest mitte-kinnipidamine ning muud sisekontrolli puudujäägid) tõttu
- **Operatsiooniriski mõõtmisel** vaadeldakse, kui suur on kindlaksmääratud ajahorisondil, kindlaksmääratud tõenäosusega, negatiivsete sündmuste kokkulangemisel ettevõtte maksimaalne kaotus.

Riskihindamise metoodika (2)

RISK

Ühekordne oodatav kahju riski realiseerumisel **x** Tõenäosuslikke riski realiseerumisi perioodis

Riskikomponendid:

Protsessi (käsitletava vara) väärtus

Ohud, nõrkused, vastu-meetmed

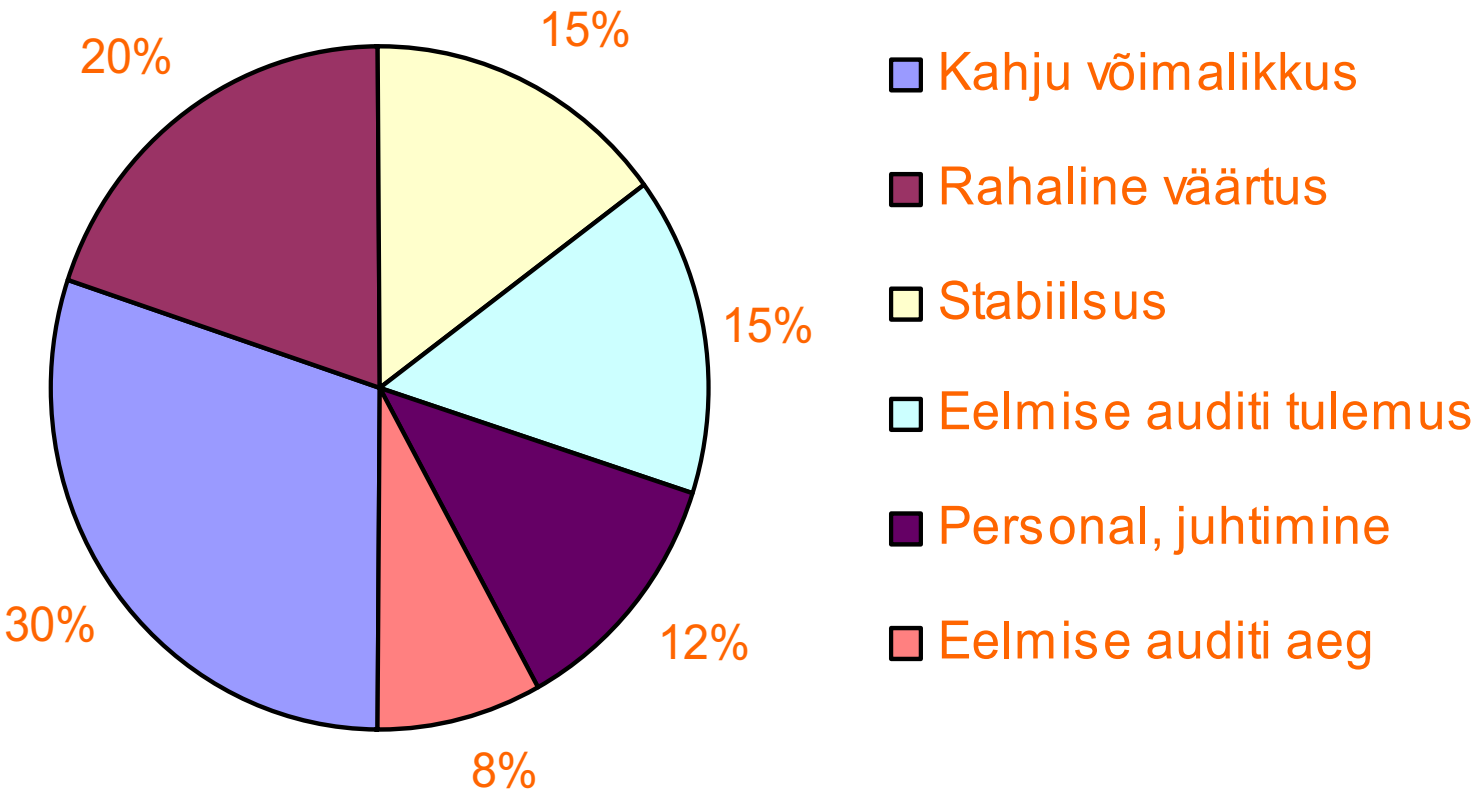
Riskifaktorid siseauditi metoodikas:

1. Kahju võimalikkus
2. Rahaline väärtus
3. Stabiilsus
4. Eelmise auditi tulemus
5. Personal, juhtimine
6. Eelmise auditi aeg

Riskifaktorid

- **Kahju võimalikkus –** iseloomustab protsessi tundlikust otsese kahju tekkele.
- **Rahaline väärtus –** iseloomustab käsitletava protsessi rahalist väärtust.
- **Stabiilsus –** iseloomustab teostatud tegevuste stabiilsust käsitletava protsessi raames
- **Eelmise auditi tulemus –** põhineb eelmise, samas valdkonnas läbiviidud auditi hinnangutel**.**
- **Personal, juhtimine –** iseloomustab juhtimise ja personali kvaliteeti
- **Eelmise auditi aeg –** arvestab kontrollide vähenemist aja möödudes

Riskifaktorid (2)



Riskitase

RISKITASE	PUNKTID	TÖÖPLAAN
Kõrge	67 - 100 punkti	Protsessi auditeeritakse vähemalt üks kord aastas
Keskmine	38 - 66 punkti	Protsessi auditeeritakse vähemalt üks kord kahe aasta jooksul
Madal	25 - 37 punkti	Protsessi auditeeritakse vähemalt üks kord kolme aasta jooksul

Siseauditi hindamismetoodika ja aruandlus

KREDIIDIASUTUSTE SEADUS

- **Siseauditi üksus** HINDAB **krediidiasutuse tavapärast majandustegevust ja sise-eeskirjade ja protseduurireeglite vastavust ja piisavust krediidiasutuse tegevusele ning kontrollib pidevalt nõukogu ja juhatuse kehtestatud eeskirjadest, protseduurireeglitest, limiitidest ja muudest normidest kinnipidamist ning jälgib Finantsinspektsiooni ettekirjutuste täitmist**

Näide:
SEB grupi hindamismetoodika

- Lähtuvalt auditeeritud PROTSESSI OLULISUSEST ning auditi käigus TUVASTATUD PUUDUSTEST sisekontrolli süsteemis, omistatakse protsessile auditi reiting – A, B, C või D
- Protsessile omistatud reiting EI OLE SAMASTATAV valdkonna reitinguga

Siseauditi hindamismetoodika

REITINGU VÕTI:

A. Sisekontrolli süsteem on efektiivsed
B. Märkused on seotud mõningaste nõrkustega sisekontrolli süsteemis
C. Olulised märkused seoses kõrge riskiga, vajalikud on kohesed muudatused töökorralduses ja sisekontrollide selge fikseerimine (näidetega kinnitatud protseduurireeglite rikkumine)
D. Kriitiline risk, sisekontrolli süsteem on puudulik (esineb olulisi kõrvalekaldeid firma poliitikast, puuduliku sisekontrolli süsteemi tõttu oht turvalisusele, tõsine oht sissetulekute vähenemiseks, varade raiskamine)

Aruandlus

- Siseauditi aruandlus tehtud tööst toimub vastavalt FIRMA NÕUKOGU poolt kinnitatud aruandlusprotseduurile.
- Aruandluse eesmärgiks on tagada informatsiooni olemasolu grupi sisekontrolli süsteemist ja selle toimimisest ning leida lahendused tekkinud küsitavustele riskide kontrollitusest lähtuvalt
- Plaanilise töö raportid edastatakse auditi lõpetamisel auditeeritud VALDKONNA JUHTIDELE
- Kord kvartalis annab siseaudit tehtud tööst aru FIRMA JUHATUSELE ja AUDITI KOMITEELE, vähemalt kord poolaastas NÕUKOGULE

Järeldused: kuidas parandada IS olukorda?
Üks võimalustest

- Teha esmane valiku COBIT 34 protsessist – näiteks 10 protsessi
- Määrata neile protsessidele omanikud/vastutajad, kes mooduvad töögrupid ja töötavad välja tööplaanid protsesside COBITile vastavuse hindamiseks – ja ettepanekute tegemiseks nende protsesside muutmiseks/täiustamiseks
- ***Kokkuvõttes: tuntud riskijuhtimise metoodika "kui ei jõua kogu rehkendust teha, siis tee pool"***

Auditi raport

Auditi Raport nr. xxx

01. september – 30. november
Koostas:
zzz
30. novembril 200x.a.

KOKKUVÕTE

OLULISED TÄHELEPANEKUD

2 OLULISED TÄHELEPANEKUD

2.1 Andmetele juurdepääsu reguleerimine – kasutajalitsentsid

2.2 Kasutajakontode haldus – portfelliõiguste andmine

2.3 Kasutajakontode haldus – muudatuste jälgimine

2.4 Sisestatavate andmete volitus- ja kontrolliprotseduurid – aegunud protseduurireeglid

2.5 Sisestatavate andmete volitus- ja kontrolliprotseduurid – muudatuste jälgimine

TEISEJÄRGULISED TÄHELEPANEKUD

3 TEISEJÄRGULISED TÄHELEPANEKUD

3.1 Andmetele juurdepääsu reguleerimine – õigustesüsteemi kirjeldus

3.2 Kasutajakontode juhtkondlik läbivaatus

3.3 Sisestatavate andmete volitus- ja kontrolliprotseduurid – kontrolltoimingute kirjeldamine

Auditi eesmärk

1.1. Auditi eesmärk

Auditi objektiks on valitud ärinõue:

– kaitsta informatsiooni volitamatu kasutamise, avalikustamise või muutmise eest ja kahjustuste või kaotsimineku eest;
– tagada andmete säilitamine täielike, täpsete ja kehtivatena nende sisestusel, värskendamisel ja talletamisel.

Riskide hindamine

1.2. Riskide hindamine

Auditeeritud protsessi riski võib defineerida kui negatiivset kõrvalekallet loodetud majanduslikust tulemusest, mis on tingitud ärieesmärkidega seotud nõuete puudumisest või süsteemi nõuetekohase toimimise järelevalve puudumisest.

Auditi ulatus

1.3. Auditi ulatus

Auditi käigus keskendutakse:

- Trema kasutajaõiguste terviklikkusele s.h. auditijälje olemasolule ja sisekontrollitoimingute piisavusele õiguste muudatuste läbiviimisel.
- Tremasse kasutajate poolt sisestatavate ja Tremasse automaatsete protsesside käigus imporditavate andmete terviklikkusele
- Sisekontrollitoimingute ja auditijälje piisavusele Trema alusandmete ja valemite (nagu hinnad, limiidid jmt) sisestamisel ja muutmisel.

Protsessi juhtimise hindamisel vaadeldakse (CobIT-i baasil):

1. Andmetele juurdepääsu reguleerimist,
2. Kasutajakontode haldust,
3. Kasutajakontode juhtkondlikku läbivaatust ning
4. Sisestatavate andmete volitus- ja kontrolliprotseduure
5. Andmetöötluse terviklikkust automaatsetes protsessides

Kokkuvõte peamistest tähelepanekutest

1.4. Kokkuvõte peamistest tähelepanekutest

Auditeeritud protsesside kontrollisüsteemide analüüsi ning läbiviidud intervjuude baasil esitatud auditi tähelepanekutest võib olulisematena välja tuua:

- mitmete tööprotseduuride ...
- puudujääke ...
- litsentsipoliitika ...

Detailsemalt on olulisi leide käsitletud raporti punktis 2.

Järeldus

1.5. Järeldus

xxx andmete haldamiseks on loodud vajalikud süsteemsed ja töötajate poolt läbiviidavad kontrollid. Süsteemi töö on olulistes lõikudes kaetud ööpäevaringse monitooringuga. Andmete sisestamiseks on kasutajatel piiratud õigused, kõrgema riskiga kohtades on rakendatud topeltkontrolle.

Probleemiks on ...

Kokkuvõte auditi käigus läbiviidud töödest

1.6. Kokkuvõte auditi käigus läbiviidud töödest

Auditi läbiviimisel tutvuti esmalt valdkonda reguleeriva dokumentatsiooniga ja kasutatavate juhtimismeetmetega, hinnati kontrollisüsteemide ja kasutatavate meetmete olulisust ning sobivust protsessi juhtimisel, vastandati kehtivat töökorraldust, kehtestatud eeskirju ja turvastandardeid ning testiti ja tõendati kehtivast juhtimiskorraldusest tulenevaid ohte ja nõrkusi.

1.6.1. Andmetele juurdepääsu reguleerimine

Juhtkond peaks kehtestama protseduurid, mis tagaksid õigeaegsed meetmed kasutajakontode muutmiseks, peatamiseks ja sulgemiseks. Nende hulka peaks kuuluma ametliku kinnituse protseduur, mis fikseerib selle, et süsteemiomanik kinnitab pääsuõigused

...

1.6.2. Kasutajakontode haldus

Juhtkond peaks evitama protseduurid, mis oleksid kooskõlas turvapoliitikaga ning tagaksid turvalise pääsu reguleerimise andmete vaatamiseks, lisamiseks, muutmiseks või kustutamiseks konkreetsetele isikutele tõendatava vajaduse põhjal.

1.6.4. Sisestatavate andmete volitus- ja kontrolliprotseduurid

Organisatsioon peaks kehtestama asjakohased protseduurid, mis tagaksid, et andmesisestust sooritaks ainult volitatud personal.

1.6.4.1. Hinnad ja valuutakursid

1.6.4.2. Uued instrumendid

1.6.4.3. Limiidid

1.6.4.4. Kontrollraportid

1.7. Juhtkonna vastused auditi raportile

Siseauditi osakond eeldab, et soovituste täitmistähtaegade määramisel peetaks kinni järgnevatest piiridest:

TÄHELEPANEKU TÜÜP	RISKI KATEGOORIA	LAHENDUSE TÄITMISE KUUPÄEV
Oluline	Kõrge	Vajalik kohene tähelepanu ja sekkumine
Teisejärguline	Keskmine, Madal	Vajalik tähelepanu ja lahenduse tähtajaline täitmine

Juhtkonna vastus raportile saabus __. _____ 2004.a.

2. Olulised tähelepanekud

2.1. ....

Tähelepanek:

…

Risk

....

Soovitus:

…

Juhtkonna vastus

…

Vastutaja: _____ _____ Tähtaeg: _____

3. Teisejärgulised tähelepanekud

3.1. ....

Tähelepanek:

...

Risk

....

Soovitus:

...

Juhtkonna vastus

…

Vastutaja: _____ _____ Tähtaeg: _____

Raporti lõpp

Raporti koostanud:	Raporti vastu võtnud:
xxxx	xxxx
Raport kooskõlastatud:	xxxx
xxxx Siseauditi osakonna juhataja	___ _____ _____ juht

Olles auditeeritav ...

Kes on audiitor?

Kes on audiitor?

Kes on audiitor?

- Ka audiitor on inimene, ta peab valideerima dokumentide, st. veenduma, et töötajad järgivad dokumentatsiooni.

Mida audiitorid teevad?

- Audiitorid analüüsivad dokumente ja poliitikaid (verifitseerimine)
- Seejärel audiitorid selgitavad, kuidas töötajad toimivad. Nad teevad kindlaks, kas kõik töötajad täidavad dokumenteeritud protseduure ja poliitikaid (valideerimine)
- Audiitorid selgitavad, kas kõik töötajad on koolitatud oma ülesannete täitmiseks

Verification:
are we building *the thing right*?

Validation:
are we building *the right thing*?

Audiitor leiab probleemi

- Kui audiitor leiab probleemi, siis ta teavitab sellest koheselt – mitteteavitamine on välistatud.
- Leiu kohta võetakse asjasse puutuvalt töötajalt allkiri.
  - Allkiri ei tähenda probleemi tunnustamist, vaid ainult fakti kinnitust
  - Kas probleem on või polnud, selgitatakse päevalõpu kohtumistel või lõppkohtumisel (*final meeting*)
- Kui audiitor ei teavita töötajat leiust, siis leidu polnud. Audiitorid ei teavita juhtkonda probleemist ilma seda eelnevalt probleemiga seotud töötajatega arutamast – "*fair play*" põhimõttest peetakse alati kinni.

Töötaja kohustused

- Töötaja peab teadma, missugune dokumentatsioon tema tegevust reglementeerib – see peab olema dokumendi viimane versioon.
- Töötaja peab teadma, mis koolitust on ta saanud – kui ei tea, küsi oma ülemuselt!
- Töötaja peab täitma kõik tema tööga seotud vormid – audiitorid kontrollivad, kas kõik on tehtud reeglitele vastavalt.

Käitumine auditi ajal

- Ole rahulik. Oota, kuni audiitor esitab küsimuse.
- Kuula tähelepanelikult küsimust, enne kui vastad. Kui sa ei saanud küsimusest aru, palu audiitoril küsimust korrata. Kui küsimus pole ikka arusaadav, siis ütle seda audiitorile.
  lialgi ära vasta küsimusele, millest sa aru ei saanud.
- **Räägi alati tõtt.** Ära püüa midagi varjata. Kui sa arvad, et varjates sa aitad kedagi, siis tea – sa ei aita. Pea meeles, et üks vale võib hävitada usalduse – ja ka kogu auditi. Usaldus kaotatakse hetkega, selle tagasivõitmine võtab aastaid.

Mida mitte teha

- Kui sa ei tea audiitori küsimusele vastust, siis ütle seda audiitorile. Ära püüa vastust võltsida/välja mõelda.
- Ära varja midagi. Kõik mida audiitor teada tahab, on see, mis tööd sa teed ja kuidas sa seda teed. Kuna seda sa tead, siis saad sellest ka vabalt audiitorile rääkida.
- Ära anna vastuseid teiste isikute eest. Kui sa tead, kes seda tööd teeb, siis teata seda audiitorile.
- Ära anna vastuseid teiste poolt tehtava töö kohta. Eeldatakse, et audiitor esitab küsimusi ainult sinu töö kohta. Kui audiitor siiski küsib teiste töö kohta, tuleb vastata: “see pole minu töö/kohustus/vastutus”.

Veel nõuandeid

- Audiitorid ei testi sinu mälu. Kui sul on vaja vaadata dokumentatsiooni, siis nii ütlegi audiitorile. Eks audiitor siis otsusta, kas sa pead mälu värskendama või ei.
- Vasta ainult küsimustele – ära anna "vabatahtlikult" informatsiooni. Audiitorit pole vaja abistada.
- Ära püüa asju selgitada, kui audiitor pole seda palunud. Las audiitor esitab küsimusi, kui miski pole talle arusaadav.